The Cybersecurity Act: Bridging Gaps in America's Cyber Defense

The threat to America's computer networks and the critical infrastructure they operate is grave and growing. A successful cyberattack against our power grid, water systems, or financial networks could have a devastating impact on public safety and wreak havoc on our economy. These dire consequences make cyberattacks a threat as serious as terrorism and other security challenges. To prevent a catastrophic attack, we must act now to bridge the security gaps that hinder our ability to defend against the evolving cyberthreat.

The Cybersecurity Act of 2012

The Cybersecurity Act of 2012 (S.3414) would bridge the gaps in our cyber defenses and help to prevent dangerous cyberattacks by establishing a robust public-private partnership and coordinated framework to protect critical infrastructure.

- **Identifying the biggest vulnerabilities.** The bill would established a National Cybersecurity Council, comprised of representatives from security and intelligence entities and chaired by the Department of Homeland Security, to conduct risk assessments and determine which sectors are subject to the greatest and most immediate cyber risk.

- **Creating public-private partnerships to combat cyberthreats.** Under the bill, industry groups would work with the Cybersecurity Council to propose voluntary, outcome-based security practices. Companies that adopt these practices would be entitled to a number of benefits including liability protection in the event of a cyberattack, expedited security clearances, priority technical assistance, and real-time threat information.

- **Improving information sharing and protection civil liberties.** Information sharing procedures in the public and private sector would be designed to ensure that privacy and civil liberties are protected.

- **Improving the security of the federal government's networks.** The bill would modernize the Federal Information Security Management Act (FISMA) and require the federal government to develop a comprehensive risk management strategy.

- **Building cybersecurity talent and tools.** The bill would reform the way cybersecurity personnel are recruited and trained, and would also coordinate cybersecurity research and development to advance the development of new security technologies.

America's Critical Infrastructure Is Vulnerable to Attack

- **America's power grids, communications lines and transportation systems are reliant on cyber networks.** Whether it is through unprotected connections between company systems to the Internet, or vulnerabilities within a company's control systems, America's critical infrastructure is dependent upon cyber networks that are vulnerable to attack.

    - As eight esteemed national security exports wrote to Senate Leadership, "The present cyber risk is shocking and unacceptable. Control system vulnerabilities threaten power plants and the critical infrastructure they support, from dams to hospitals." [Letter from national security experts, 1/19/12]

    - Former Homeland Security Sectary Michael Chertoff notes, "[I]n an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems." [Michael Chertoff Statement, 2/14/12, letter here]

- **Critical infrastructure networks are *already* under attack, and vulnerabilities are growing.** In just the past two years, cyberattacks on critical infrastructure in the U.S. have increased dramatically. In 2009, nine cyberattacks on critical infrastructure facilities were reported to the Department of Homeland Security (DHS). In 2011, that figure skyrocketed to 198 reported attacks. [*CNN Security Clearance*, 7/4/12]

- **Weak cyber policies undercut American strength.** "In the new global competition, where economic strength and technological leadership are as important to national power as military force, failing to secure cyberspace puts us at a disadvantage…. America's power, status, and security in the world depend in good measure upon its economic strength; our lack of cybersecurity is steadily eroding this advantage." [CSIS, 12/08]

America is Ill-Equipped to Defend Against Cyberthreats

- **Existing cyber polices are riddled with holes, overlapping missions, and inadequate coordination between entities.** In 2008, the White House conducted a sixty day cyberspace policy review and concluded: "The Federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way." [CSIS, 12/08; White House Cyberspace Policy Review]

- **The U.S. has no clear chain of command for issuing, implementing and coordinating threat prevention standards or responses to an attack.** A number of different agencies have overlapping missions and there is weak coordination between them. As a result, the U.S. maintains a patchwork of ad hoc, incoherent cyber policies that undermine the government's ability to prevent and respond to a major cyberattack. Countless government and private sector reports have urged Congress to update legal authorities so the government can properly prevent and mitigate an attack, including:

- Secretary Napolitano: "DHS must execute its portion of the cybersecurity mission under an amalgam of existing statutory and executive authorities that fail to keep up with the responsibilities with which we are charged…our nation cannot improve its ability to defend against cyberthreats unless certain laws that govern cybersecurity activities are updated." [Testimony of Secretary Napolitano, 2/16/12]

- The White House in its *Cyberspace Policy Review*: "Answering the question of "who is in charge" must address the distribution of statutory authorities and missions across departments and agencies…. Unifying mission responsibilities that evolved over more than a century will require the Federal government to clarify policies for cybersecurity and the cybersecurity-related roles and responsibilities of various departments and agencies." [White House Cyberspace Policy Review]

- 9/11 Commission Co-Chairs Tom Kean and Lee Hamilton: "Much like the situation before the September 11th, 2001, attacks, the federal government is not adequately organized to deal with a significant emerging national security threat…. Comprehensive legislation is needed to flesh out a range of pressing cyber security policy questions, including how the federal government should defend against and respond to cyber attacks." [Letter from Co-Chairs Kean and Hamilton, 3/5/12]

- **The Federal Information Security Management Act (FISMA) is out of date and in desperate need of reform.** [CSIS, 12/08]

  - In 2002, FISMA was enacted to improve network security by strengthening previous safeguards, creating a framework for security investment, and reporting on agency performance in meeting security benchmarks. However, cybersecurity demands continuous monitoring of government networks for threats and vulnerabilities, rather than the once-a-year audits required under current law.

  - As CSIS notes, "FISMA was not designed to provide minute-by-minute views into network security. To some in government and industry, FISMA has become a paperwork exercise rather than an effective measure of network security…. FISMA lacks effective guidance and standards for determining appropriate levels of risk; it lacks requirements for testing or measuring an agency's vulnerabilities of its plans for mitigating such vulnerabilities; it fails to define agency responsibilities for effective controls over contractors or vendors; and it does not recognize the emergence of new technologies and network architectures."

Action is Needed to Shore Up America's Cyber Defense

- **Improved information sharing between government and the private sector is needed.** Creating a common operating picture through information sharing will allow network operators to see the full range of threats facing networks and react in real time. As the White House Cyberspace Policy Review explains, "Businesses need effective means to share detection methods, information about breaches and attack methods, remediation techniques, and forensic capabilities with each other and the Federal government." Timely information is crucial "to preventing, detecting, and responding to cyber incidents." [White House Cyberspace Policy Review; Testimony of DNI Clapper, 1/31/12]

- **Enhancing research and development will build America's cyber defenses and boost American industry.** Art Coviello, Executive Chairman of leading computer security firm RSA, has stated that, "Many security technologies are past their freshness date – offering diminished value….We need to adopt the security innovations already developed and being developed to keep pace with the innovations in information technology and escalating threats." Strong research and development initiatives will be essential to building innovative technologies that will strengthen the nation's cyber defenses. [RSA Executive Chairman Art Coviello's remarks]

- **American companies have an opportunity to corner the cybersecurity market.** In the 1940s, Defense Department research and development helped to make our Armed Forces the best in the world and strengthened American industry. Incentives to secure the Internet will create demand for cutting edge products to stay ahead of evolving threats, and will drive the market and spur further advancement in the field. Security will improve and American innovators and companies producing the technologies will reap the benefits. [CSIS, 12/08]

- **America must make cybersecurity careers attractive to young talent.** High schools and universities need more computer science programs to spur the interest and build the skills in American students to become the next generation of cybersecurity professionals. An American workforce equipped with the skills and drive to succeed and continuously innovate is necessary to secure the future. Like the period after the launch of the Sputnik satellite in the 1950s, the United States is now engaged in a global race that relies on science and mathematics skills. [White House Cyberspace Policy Review; CSIS, 12/08]